JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE **Noted: October 30, 2015** ***[Evidentiary Hearing Requested]***

I. MOTION

Jay Michaud, through his counsel Colin Fieman and Linda Sullivan, respectfully moves the Court pursuant to Fed. R. Crim. P. 12(b)(3)(c) for an order suppressing all evidence obtained from the Government's deployment of a "Network Investigative Technique," a surreptitious computer hacking method, on Mr. Michaud's private computer. Mr. Michaud also seeks suppression of all fruits of the Government's illegal search, including any allegedly inculpatory statements by Mr. Michaud.

Mr. Michaud has been charged with receipt and possession of child pornography, in violation of U.S.C. §§ 2252(a)(2), (a)(4) and (b)(1). Trial is scheduled for February 16, 2016.[1]

[1] The pretrial motion deadline is January 28, 2016. At this time, the discovery process is continuing and, among other evidence, the defense has not yet received a copy of the programming code for the NIT or mirror image copies of the data storage devices that were seized by the Government. Given this pending discovery and investigation, the defense reserves the right to supplement its suppression motion.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

II. STATEMENT OF FACTS

On July 10, 2015, FBI agents assisted by local law enforcement executed a search warrant at the home of Jay Michaud in Vancouver, Washington. Mr. Michaud is 62 years old and worked as an administrative employee of the Vancouver School District. He has no criminal history. The search was conducted pursuant to a warrant issued by the Hon. David Christel on July 9, 2015. The warrant was based on an application prepared by FBI Special Agent Samuel Mautz. Exh A ("the Residential Warrant").

As set forth in that application, the events leading to the search of Mr. Michaud's home began on or about February 20, 2015, when the FBI took control of a web site identified as "Website A" based in Virginia. Exh. A at ¶ 11. Website A is described as a "child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children." *Id*. Based on the discovery and defense investigation to date, it appears that Website A offered a mix of discussion forums, private messaging services, both legal and illegal pictures and videos, and links to pictures and videos. *See also id*. at ¶ 15. As of March 4, 2015, the site had 214,898 "members." *Id*. at ¶ 12. The discovery further indicates that site members resided throughout the United States and, most likely, many places abroad. Users accessed the site with a username and password, and they were instructed to avoid using personally identifying information when joining or communicating on the site. *Id*. at ¶¶ 12-13.

In addition, Website A operated on a network that is designed to protect user privacy and "facilitate anonymous communication over the Internet." *Id*. at ¶ 7. This network is commonly known as "the onion router" or "Tor" network, and is designed to route communications through multiple computers to protect the confidentiality of the internet protocol (IP) addresses and other identifying information of its users. *See id*. at

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

¶¶ 7-10; *see also* https://www.torproject.org ("Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security."). The network was originally designed by the U.S. Naval Research Laboratory and is freely available to the public. The network is readily accessed by downloading free software and, like the Internet in general, it can be used for both legitimate and illicit purposes. *See* James Ball, *Guardian Launches Secure Drop System for Whistleblowers to Share Files*, The Guardian, June 5, 2014 (describing the newspaper's initiation of a secure means for whistleblowers to submit documents via the Tor network);[2] Virginia Heffernan, *Granting Anonymity*, N.Y. Times, December 17, 2010 ("Peaceniks and human rights groups use Tor, as do journalists, private citizens and the military, and the heterogeneity and farflungness of its users — together with its elegant source code — keep it unbreachable.").[3]

In this case, it appears from the discovery that a foreign law enforcement agency first identified Website A in December, 2014, and provided the FBI with an IP address associated with the site. *See* exh. B ("the Title III warrant") at ¶ 38. This IP address had been captured during a period when there was a brief "misconfiguration of the server" that hosted the site, allowing investigators to collect site address information that would not normally have been publicly accessible. *Id*. Following up on this information, the FBI identified and arrested the administrator of the site in February, 2015. The FBI then took control of the site and continued to operate it for investigative purposes.

To this end, on February 20, 2015 the FBI obtained authorization pursuant to 18 U.S.C. § 2518 (commonly referred to as "Title III" or "the Wiretap Act") to intercept

[2] Available at: http://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents

[3] Available at: http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html?_r=0

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

electronic communications on the "target site's" private chat and messaging services between unknown "target subjects" or "unidentified administrators and users." Exh. B at ¶ 3.[4] This authorization was apparently sought because 18 U.S.C. § 2511 generally prohibits electronic communication service providers from monitoring communications on their services, and the FBI had become the service provider for the child pornography site.

In its wiretap application, the Government disclosed that, in conjunction with its interception of chats and messages, it would deploy a "Network Investigative Technique" (NIT) that would work in the following way:

> The NIT will send one or more communications to TARGET SUBJECTS that access the TARGET WEBSITE after the date of its deployment, which communications are designed to cause the computer receiving it (sic) to deliver data that will help identify the computer, its location, other information about the computer, and the user of the computer accessing the TARGET WEBSITE. In particular, the NIT is designed to reveal to the government the computer's actual IP address. . . and other information that may assist in identifying computers that accesses (sic) the TARGET WEBSITE and their users.

Exh. B at ¶ 53. The Wiretap application goes on to note that the FBI would seek a separate search warrant for "deployment" of the NIT. *Id*.

Accordingly, on the same day, the FBI submitted a search warrant application ("The NIT Application") to Magistrate Judge Theresa Carroll Buchanan in the Eastern District of Virginia. Exh. C. This application sought authorization to use the NIT to search any and all "activating computers," which are the computers "of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." Exh. C at Bates 136 ("Attachment A"). The warrant application further stated that the NIT would seize information from the target computers that included

[4] "Website A" referenced in the Residential Application and the "Target Website" referenced in the Title III Application are the same.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

their IP addresses; the type of operating systems on the computers; and whether the "NIT has already been delivered to the activating computer." *Id*. at Bates 137 ("Attachment B"). Elsewhere in the application, the NIT is broadly described as "computer instructions" that would be unknowingly downloaded by the unidentified target users when they access the site. Exh. C at ¶ 33.

The application further states that "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation" the NIT may be deployed against "any user who logs into the TARGET WEBSITE," regardless of the nature or extent of their activities in connection with the site. Exh. C at Bates 161, n. 8. While the application goes on to state that the FBI may elect to target particular users "more discretely," *id*., it sought and obtained authorization to deliver the NIT to all of the tens of thousands of site members, regardless of their location or whether they are merely engaging in chat or bulletin board communications that did not involve the receipt or distribution of illegal images.

Further, the NIT application does not allege that anyone who visited the Target Website necessarily viewed or downloaded illegal pictures. In this regard, the application does not claim that the name of the site identifies it as a source of child pornography, and while the main page contained "two images depicting partially clothed prepubescent girls with their legs spread apart," exh. C at ¶ 12, the application does not claim that these images are child pornography. The rest of the main page consists of instructions for registering an account and related information. *Id.* Moreover, once a user enters the site, he or she is presented with a variety of forums, including various chat rooms, "general discussion" and "security and technology" forums, and more explicitly labeled sections for such things as "Pre-Teen Videos" and "HC" (hardcore). Exh. C at ¶¶ 14-17.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Finally, the FBI requested authorization to delay providing notification to the targets of the NIT search for a period of "30 days after any individual accessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure." Exh. C at ¶ 40. The court granted this request for a period not to exceed 30 days and, from the available discovery, it appears that no extension of this delayed notice was requested or granted. *See* exh. C at Bates 135.

The FBI began "deploying" its NIT on February 20, the same day the NIT warrant was granted. It appears from the discovery available to date that, in order to avoid revealing to potential targets that it had taken control of Website A, the FBI continued to distribute child pornography from the site. *See* Exh. B at ¶ 61 ("In order to ensure that users continue to access the TARGET WEBSITE, it is necessary that there be as minimal an interruption as possible in the operation of the TARGET WEBSITE, so as not to create suspicion among the TARGET SUBJECTS that a law enforcement action is taking place on the board"); Exh. A (Residential Warrant) at ¶¶ 30-32 (stating that during the time the site was controlled by the Government a user later identified as Mr. Michaud accessed posts on the site that contained links to illegal videos); Dkt 1 (Complaint) at ¶ 12 (describing an image allegedly accessed by Mr. Michaud on the site during the time the FBI controlled it).

On or about February 28, the FBI surreptitiously sent the NIT to a computer connected to someone with the user name "Pewter" and extracted its IP address and other identifying information. According to the July 8, 2015, application for a warrant to search Mr. Michaud's home, "Pewter" had accessed posts on the Target Website on February 28 and March 2 that contained links to child pornography videos. Exh. A at ¶¶ 25-28. In addition, the residential application alleged that "Pewter" had previously been logged into the site for 99 hours and had viewed 187 message threads with explicit

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

conversations about child pornography and links to additional files and comments. *Id.* at ¶ 26. It appears from the discovery that none of this information was known to law enforcement before the NIT was deployed against "Pewter."

On March 9, 2015, the FBI sent an administrative subpoena to Comcast for information related to the "Pewter" IP address that – through use of the NIT – had been seized on February 28 and March 2. Comcast responded the same day with Mr. Michaud's subscriber information, including his telephone number and address. *See* Exh. D. [5]

On the morning of July 10, 2017, FBI agents made contact with Mr. Michaud outside a Starbucks near his home. The agents advised him that they had the Residential Warrant issued by Judge Christel, but they did not disclose that his computer had previously been searched or provide him with a copy of the NIT warrant. Mr. Michaud cooperated with the agents and gave them the keys to his apartment. Following a search of Mr. Michaud's home and vehicle, agents arrested him and seized his personal computer, phone, CD's and other digital storage devices and personal property.

Later the same day, the Government filed a complaint with this Court, charging possession of child pornography. Dkt. 1. The complaint did not disclose the Title III warrant or the fact that Mr. Michaud's computer had been searched by means of the NIT in February. Instead, the sworn Complaint stated that "*using publicly available websites*, FBI special agents were able to determine" that a computer with the IP address associated with Mr. Michaud had accessed images on the site. *Id*. at ¶ 13 (emphasis added); *see also id*. at ¶ 8 (noting that "further law enforcement

[5]Mr. Michaud moved to a new address in Vancouver in May, 2015. Comcast provided this new address to the FBI on June 17, 2015.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

investigation" led to identification of Mr. Michaud's IP address, with no mention of the NIT or search of his computer).

On July 14, 2015, defense counsel served the Government with a comprehensive discovery request, including a request for "copies of any search warrants and affidavits resulting in the seizure of evidence intended for use by the government at trial." On August 19, 2015, the Government disclosed the existence of the NIT warrant by providing a copy of it to the defense. The Title III warrant was not disclosed until October 6, 2015, following supplemental discovery demands by the defense.

III. ARGUMENT

The Government's search of Mr. Michaud's computer, and apparently myriad other computers, was undertaken in blatant violation of the jurisdictional and particularity requirements for searches imposed by Fed. R. Crim. P. 41. These restrictions are not mere technicalities. Instead, the Rule serves as a critical bulwark against the very type of sweeping, dragnet searches and unrestrained Government surveillance that occurred in this case. Consistent with the core Fourth Amendment purposes served by Rule 41, the law is clear that suppression is the appropriate remedy to both vindicate Mr. Michaud's constitutional rights and curtail the Government's "NIT" hacking program.

A. The Warrant Violated Rule 41

The search of Mr. Michaud's home is the result of illegal Governmental infiltration of private computers throughout the United States and, most likely, numerous other countries. In conjunction with the continued operation of an illicit web site, the Government knowingly circumvented the limits clearly established by Fed. R. Crim. P. 41 on its ability to conduct borderless dragnet searches. The scope of this intrusion and the long term privacy implications of the Government's methods, if approved by this Court, can hardly be overstated. *See generally*, Kevin Poulsen, *Visit*

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the Wrong Website, and The FBI Could End Up in Your Computer, Wired.com, August 5, 2014 (although targeted use of "malware" by the FBI is not new, "[w]hat's changed is the way the FBI uses its malware capability, deploying it as a driftnet instead of a fishing line").[6] Fortunately for Fourth Amendment purposes, the law is clear that the type of violation that occurred in this case requires suppression of all evidence that is the fruit of that violation.

Specifically, Rule 41(b) provides authority to a magistrate judge to issue a warrant in five different situations:

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property *located within the district*;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property *outside the district if the person or property is located within the district when the warrant is issued but might move or be moved* outside the district before the warrant is executed;
>
> (3) a magistrate judge—*in an investigation of domestic terrorism or international terrorism*—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant *to install within the district a tracking device*; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, *but within any of the following*:

---

[6] Available at: http://www.wired.com/2014/08/operation_torpedo/

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

(A) a United States territory, possession, or commonwealth;

(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

The warrant in this case is not authorized under any of these sections and is therefore plainly unlawful. In a recent case involving similar methods, the court in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) ("*In re Warrant*") reached the same conclusion and refused to issue a warrant.[7] There, the Government was investigating a fraud and identity theft case perpetrated by unknown persons with a computer in an unknown location. *Id*. at 755. Like the warrant here, the warrant sought in that case would have "surreptitiously install[ed] data extraction software" on a computer somewhere in the world, causing that computer to transmit identifying information to FBI agents in the district where the warrant was requested. *Id*.

The *In re Warrant* warrant was both broader and narrower than the one in Mr. Michaud's case. It was broader in that it sought authorization "not only to extract certain stored electronic records but also to generate user photographs and location information[.]" *Id.* at 755. However, the breadth of the search was not part of the court's analysis under Rule 41. The request was also narrower than that here, because it

[7] There is a dearth of opinions addressing the legality of the Government's computer hacking programs and other high-tech surveillance methods, in part because it has often masked its use of intrusive search technology from judges. *See, e.g.,* Nicky Woolf, *2000 Cases May be Overturned Because Police Used Secret Stingray Surveillance,* The Guardian, September 4, 2015 (reporting on wide spread discovery violations and misrepresentations to local courts by police and prosecutors who had signed agreements with the FBI not to disclose their use of secret cell phone tracking technology); available at: http://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

was aimed only at one particular computer that had allegedly been involved in identity theft, rather than at any computer in the world that logged onto the "Target Website."

1. The Warrant is Not Authorized Under Rule 41(b)(1).

In *In re Warrant*, the Government sought the warrant under Rule 41(b)(1), which "allows a 'magistrate judge with authority in the district ... to issue a warrant to search for and seize a person or property located within the district.'" *In re Warrant,* 958 F. Supp. 2d at 756 (quoting Rule 41). The Government relied on Rule 41(b)(1) because, while the location of the target computer was unknown, it maintained that the property to be searched was located in the district where the warrant would be issued (the Southern District of Texas). *Id*. Although the Government conceded that the location of the target computer was unknown, its theory was that "this subsection authorizes the warrant 'because information obtained from the Target Computer will first be examined in this judicial district.'" *Id*. (quoting warrant).

Not surprisingly, the court rejected the Government's novel theory that a search did not occur until investigators received and examined information that had been extracted from the target computer. "Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location." *Id*. at 757. The search and seizure of data occurs "not in the airy nothing of cyberspace, but in physical space with a local habitation and a name." *Id*.; *see also generally id.* at 756-57 (noting that Rule 41(a)(2)(A) defines 'property' subject to search and seizure to include 'information,' and that courts have long held that 'property' under Rule 41 includes computer data.).

Accordingly, the warrant sought by the Government would have permitted "FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district." *Id.* Since the search for

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

and collection of information would occur on a Target Computer that may be outside the district, the court had little difficulty concluding that it was not authorized under Rule 41(b)(1), regardless of where seized data was examined.

In this case, presumably in response to *In re Warrant*, the Government was much more misleading about its targets, but ultimately got caught up in its own obfuscations. In the NIT warrant application, the Government baldly asserted that it sought authorization to search a "person or property in the Eastern District of Virginia." Exh. C at Bates 134-35. It is only upon a close reading of the warrant application that it becomes clear that the Virginia server for the "Target Website" was already under the control of the FBI, and the actual "place to be searched" was not the server, but the various "activating computers" that would be forced to send data to that server at the prompting of a NIT. If there were any doubt about this, the Government itself slipped up later in the application by listing "activating computers," regardless of their location, as the "place" from which information will be collected, and the "information to be seized" as various information seized "*[f]rom* any 'activating computer.'" Exh. C at Bates 169 ("Attachment A: Place to be Searched") (emphasis added); *see also* Exh. B (Title III Warrant) at ¶ 71 ("It is not presently known with any certainty where any of the remaining TARGET SUBJECTS reside").

Hence, even though the initial step in conducting the NIT searches and seizures involved the FBI's surreptitious delivery of computer code to target computers from a server in Virginia, and the data seized by the NIT was sent back to that server, there can be no credible dispute that the actual searches occurred when the NIT was installed on Mr. Michaud's and other target computers and information was extracted from them. Calling the Virginia server the "place to be searched" is therefore akin to claiming that the search of a Tacoma home pursuant to a Virginia warrant actually occurs in Virginia, so long as the executing agents are based in Quantico. *See also* Exh. A (Residential

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Application) at ¶ 24 (the NIT caused target computers "to deliver" data to a computer "controlled by the government").

In short, the *In re Warrant* court squarely concluded that "the Government's application cannot satisfy the territorial limits of Rule 41(b)(1)." *Id.* at 757. There is no meaningful distinction between the warrant in that case and the one now at issue, and the statement applies just as strongly here.

2. The Warrant Is Not Authorized Under Any of the Other Subsections of Rule 41(b).

Having concluded that a warrant to search computers in unknown locations is not allowed under Rule 41(b)(1), the *In re Warrant* court turned to the other subsections of Rule 41. It noted that Rule 41(b)(2), which deals with transient targets, actually bolsters the conclusion regarding Rule 41(b)(1):

> This subsection allows an extraterritorial search or seizure of moveable property "if it is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." FED.R.CRIM.P. 41(b)(2). Note that (b)(2) does not authorize a warrant in the converse situation—that is, for property outside the district when the warrant is issued, but brought back inside the district before the warrant is executed. A moment's reflection reveals why this is so. If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found.

Id. at 757.

Nor does the warrant application in this case come within (b)(3), as this is not a terrorism investigation.

Subsection (b)(4) deals with tracking devices. Even if the NIT were deemed comparable to a tracking device (though there is no credible basis for treating it as such), this subsection does not apply here. As discussed in *In re Warrant*, "there is no showing that the installation of the 'tracking device' (i.e. the software) would take place

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet." *Id.* at 758.

Finally, subsection (b)(5) authorizes a "magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia" to issue a warrant for property outside the district. However, this provision only applies when the property is located in certain specified areas (such as United States territories or diplomatic missions), none of which are applicable here.

Of course, *In re Warrant* is not controlling precedent. But its analysis is not just persuasive, it follows directly from the plain wording of Rule 41 and from the nature of what the warrant in that case authorized. The conclusion is as manifest here as it was in *In re Warrant*: "the Government's application cannot satisfy the territorial limits" of Rule 41." *Id.* at 757.

B. The Violation of Rule 41 Requires Suppression.

The court in *In re Warrant* refused to issue a warrant that violated Rule 41 and therefore did not address the question of what remedy is required when a warrant has been improvidently issued in violation of the Rule. In this case, the law is clear that suppression is the required remedy.

> Suppression of evidence obtained through a search that violates Federal Rule of Criminal Procedure 41 is required only if: 1) the violation rises to a 'constitutional magnitude;' 2) the defendant was prejudiced, in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule; or 3) officers acted in 'intentional and deliberate disregard' of a provision in the Rule.

United States v. Weiland, 420 F.3d 1062, 1071 (9th Cir. 2005).

Although running afoul of any one of these prongs requires suppression, the Government in this case has achieved a trifecta. First, the Government's violation of Rule 41 is of constitutional magnitude because it did not involve mere ministerial violations of the rule. *See, e,g,, United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2014) (the language of Rule 41(b)(2) is "crystal clear" and a "jurisdictional flaw" in the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

warrant cannot be excused as a "technical defect."). To the contrary, courts have long recognized that protection of the home, where Mr. Michaud used his computer, and maintaining the privacy of the personal "papers and effects" now commonly stored on computers, lies at the heart of the guarantees afforded by the Fourth Amendment. *See, e.g., Payton v. New York*, 100 S. Ct. 1371, 589–90 (1980); *accord, United States v. Becker*, 23 F.3d 1537, 1539 (9th Cir. 1994) ("[t]he sanctity of a person's home, perhaps our last real retreat in this technological age, lies at the very core of the rights which animate the [fourth] amendment"). Moreover, allowing the Government to ignore the limits imposed by the Rule will invite further violations and undermine the core constitutional requirement that warrants particularly describe the place or places to be searched. *See In re Warrant*, 958 F. Supp. 2d at 758 ("This particularity requirement arose out of the Founders' experience with abusive general warrants").

In regard to the second independent basis for suppression, Mr. Michaud certainly was prejudiced "in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule[.]" *Weiland*, 420 F.3d at 1071. Again, the Government's actions are not mere technical violations that had no bearing on the legality or outcome of the search. Had the Government complied with the territorial limits of Rule 41, it would have searched only "activating computers" in the Eastern District of Virginia. Therefore, "the search would not have occurred," meaning Mr. Michaud was prejudiced and that suppression is required. *See also, e.g., United States v. Krueger*, 998 F. Supp. 2d 1032 (D. Kan. 2014) (where Government obtained warrant in Kansas for a house in Oklahoma where Kansas resident was visiting, the "court finds that defendant has shown prejudice in that if Rule 41(b)(2) 'had been followed to the letter'" the warrant would not have been issued and that this prejudice required suppression).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Third, the officers acted in intentional and deliberate disregard of Rule 41. There is simply no credible way to interpret the Rule that would allow dragnet searches of computers outside the authorizing district. This conclusion is self-evident from the plain language of the Rule, even without reference to the decision *In re Warrant*, and it is unlikely that the Government will claim that it was unaware of that opinion when it fashioned the Virginia NIT application. Because the Government acted with intentional and deliberate disregard of the territorial limits of Rule 41, suppression is also required on this basis. *See also United States v. Gantt*, 194 F.3d 987, 1005 (9th Cir.1999), *overruled on other grounds by United States v. W.R. Grace*, 526 F.3d 499, 506 (9th Cir. 2008) (because agents' refusal to provide warrant to its subject was deliberate, court did not need to "consider whether the violation was 'technical' or 'fundamental'"; "Our Rule 41(d) jurisprudence requires suppression under these circumstances"); *United States v. Slaey*, 433 F. Supp. 2d 494, 499 (E.D. Pa. 2006) (suppressing evidence when prosecutor obtained magistrate authorization not to leave unsealed attachments to the warrant with the subject because "it was not reasonable for the agent to rely on a Magistrate Judge's order authorizing him to disregard Rule 41(f)(3)(B)").

C. The Government's Deliberate Violation of Rule 41's Notice Requirements Also Supports Suppression.

Finally, the Government's disregard for the limits imposed by Rule 41 is compounded by its violation of both the rule's and the NIT warrant's explicit notice requirements. Rule 41(f)(1)(C) requires notice by mandating that the officers give a copy of the warrant to the person from whom property was taken or else leave a copy at the place from which they took property. Rule 41(f)(3) allows courts to authorize the Government to delay notifying the target of a search that his or her property has been searched if such delay is "authorized by statute."

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In this case, the Government relied in the NIT warrant application on 18 U.S.C. § 3103a(b), which allows for delayed notice of a search of electronic information if the issuing court finds, *inter alia*, that immediate disclosure would seriously jeopardize an investigation. *See* 18 U.S.C. §§ 3103a(b)(a) and 2705; Exh. C at ¶¶ 38-41. The Virginia court authorized the Government in the NIT warrant to delay notification for up to 30 days following execution of the NIT on a target computer. Exh. C at Bates 135. There is no record in the discovery provided to date showing any request for an extension of that notification period or authorization for additional delay.

Nevertheless, although Comcast had informed the FBI of Mr. Michaud's name and address on March 9 (*see* exh. D), the Government did not provide notice of the NIT search to him until it turned over a copy of the NIT warrant to defense counsel on August 19, more than five months after the search. Indeed, the Government took pains to delay disclosure for as long as possible, going so far as to conceal the NIT search from Mr. Michaud when it filed the Complaint against him on July 10, 2015. *See* Dkt. 1 at ¶ 13 (averring that Mr. Michaud's IP address had been identified by means of "publicly available websites" and conspicuously failing to disclose that it was actually acquired by means of a computer search or refer to the NIT).

While it is unclear in this Circuit whether a deliberate violation of Rule 41's notice requirements *standing alone* still requires suppression, the notice violation in this case, at a minimum, further demonstrates the Government's deliberate disregard for the requirements of Rule 41and the Fourth Amendment. The Supreme Court has long held that "the common law principle of announcement [of a search] is 'embedded in Anglo-American law'" and "is an element of the reasonableness inquiry under the Fourth Amendment." *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995) (citation omitted). Consistent with this principle, the Ninth Circuit has held that Rule 41's notice and service requirements "must be interpreted in the light of the important policies

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

underlying the warrant requirement," including assuring property owners of a search's legality and restraining the police. *Gantt*, 194 F.3d at 990-91 (discussing former Rule 41(d), amended and moved in 2002 to Rule 41(f)(c)). Where, as here, the available evidence demonstrates a "deliberate disregard" of Rule 41's notice rules and the time limits in the NIT warrant itself, suppression is required. *Gantt*, 194 F.3d at 1005; *see also United States v. Ridgway*, 300 F.3d 1153, 1158 (9th Cir. 2002) (remanding for district court to determine whether there was a failure to serve part of warrant and, if so, whether failure was deliberate or prejudicial); *United States v. Conte*, No. CR 04–0044 SI, 2004 WL 2988567, at *5 (N.D. Cal. Dec. 28, 2004) (granting evidentiary hearing on whether there was proper service of warrant and, if not, whether violation was deliberate or prejudicial).

It is important to note that several recent cases have suggested that the holding in *Gantt* should be revisited. *See United States v. Williamson*, 439 F.3d 1125 (9th Cir. 2006) (declining to suppress for "technical" error in providing notice because failure was not deliberate, and noting that "that several post-*Gantt* cases cast doubt on *Gantt*'s status as good law"). However, *Gantt* remains the law in this circuit. In addition, regardless of whether a deliberate notice violation requires suppression in the absence of other deliberate or prejudicial violations of Rule 41, the violation is nonetheless relevant to the Court's consideration of whether the Government has engaged in a pattern of flouting the Rule and whether the NIT search was reasonable. The notice violation also bolsters the conclusion that the Government's violation of rule 41(b) was deliberate, in which case suppression is indeed required.

///

///

///

///

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

IV. CONCLUSION

The Court should order all fruits of the NIT warrant suppressed, including the warrant for Mr. Michaud's computer and all fruits of that warrant.

Dated this 16th day of October, 2015.

Respectfully submitted,
s/ Colin Fieman
s/ Linda Sullivan
Assistant Federal Public Defenders

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on October 16, 2015, I electronically filed the foregoing Motion and Memorandum in Support of Motion to Suppress Evidence, Affidavit of Colin Fieman and Proposed Order with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered with the CM/ECF system.

s/ *Amy Strickling*
Amy Strickling, Paralegal
Federal Public Defender Office
1331 Broadway, Suite 400
Tacoma, WA 98402
253-593-6710 voice
253-593-6714 facsimile